RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART2-R03

AI-Driven Exposure Management: The Path to Self-Healing Systems

Tyler Shields
Principal Analyst, Risk and Security
Enterprise Security Group

Dave Gruber
Principal Analyst, Security Operations
Enterprise Security Group

Is This You?

- Your board wants to see the latest RISK METRICS
- Threats and exposures keep you up at night… afraid of the next HACK

UGH… Why did I take this job in the first place!

Why Can’t THIS Be You Instead?!

What You WANT!

- Complete asset and risk visibility
- Prioritized risk reduction with full contextual knowledge
- Continuous validation of remediation and new findings
- NO FALSE POSITIVES
- NO FALSE NEGATIVES
- Automated remediation

Precognition of attack and preventative security

RSAC™ 2025 Conference

How Did We Get Here?

Risk Management Is Increasing In Difficulty

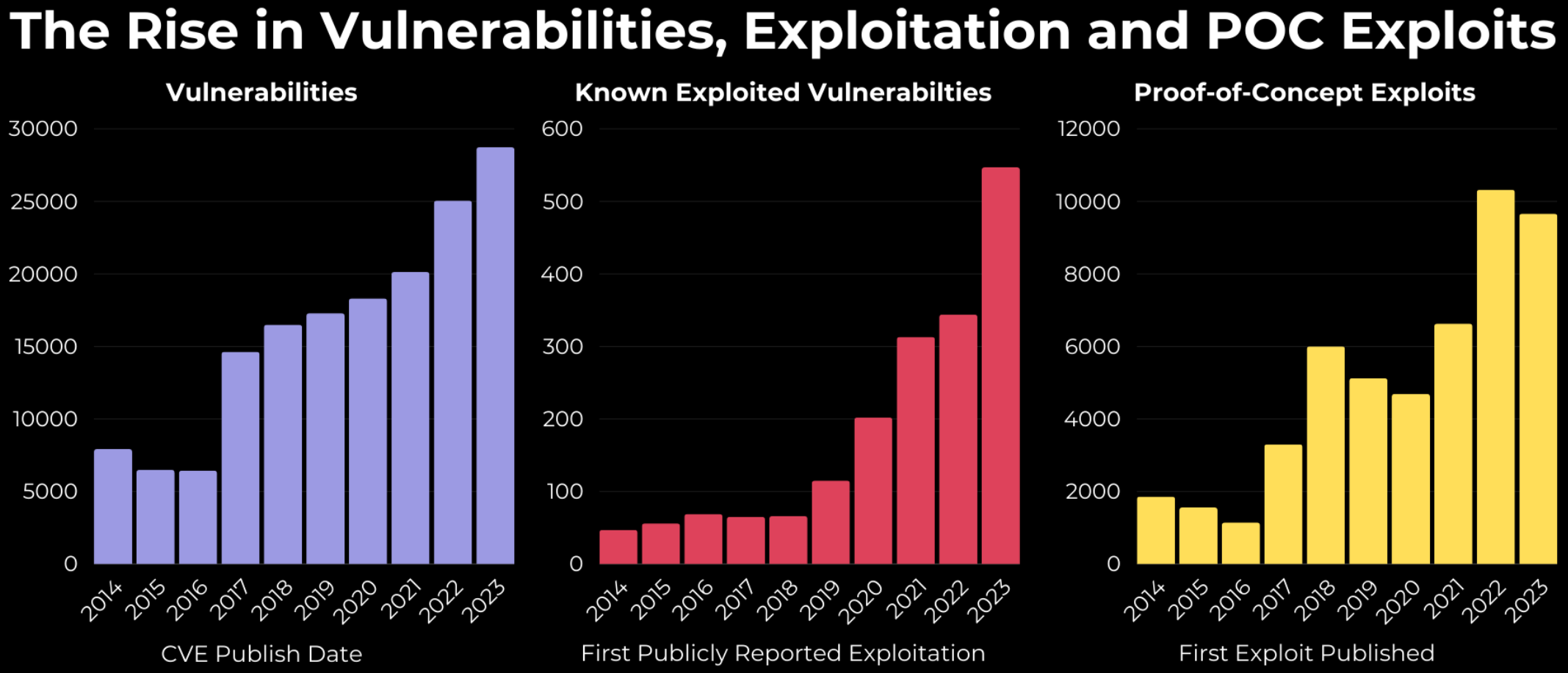
65%

Cyber-risk management is at least somewhat more difficult than it was two years ago

Which of the following best describes your organization's process for assessing its overall cyber-risk posture? (Percent of respondents, N=375)
47%
27%
9%
13%
3%
My organization has a defined process to assess its overall cyber-risk posture, and it is always followed completely
My organization has a defined process to assess its overall cyber-risk posture, but it isn't always followed completely
My organization has some guidelines to assess its overall cyber-risk posture but not a defined process
My organization assesses its cyber-risk posture on a fractional or partial basis
My organization currently does not assess its cyber-risk posture in any capacity

Enterprise Strategy Group - Cyber Risk Management Survey 2024

If we don’t become proactive, we will drown…



Source: VulnCheck Blog State of Exploitation – A Peek into the Last Decade of Vulnerability Exploitation Dated May 2024

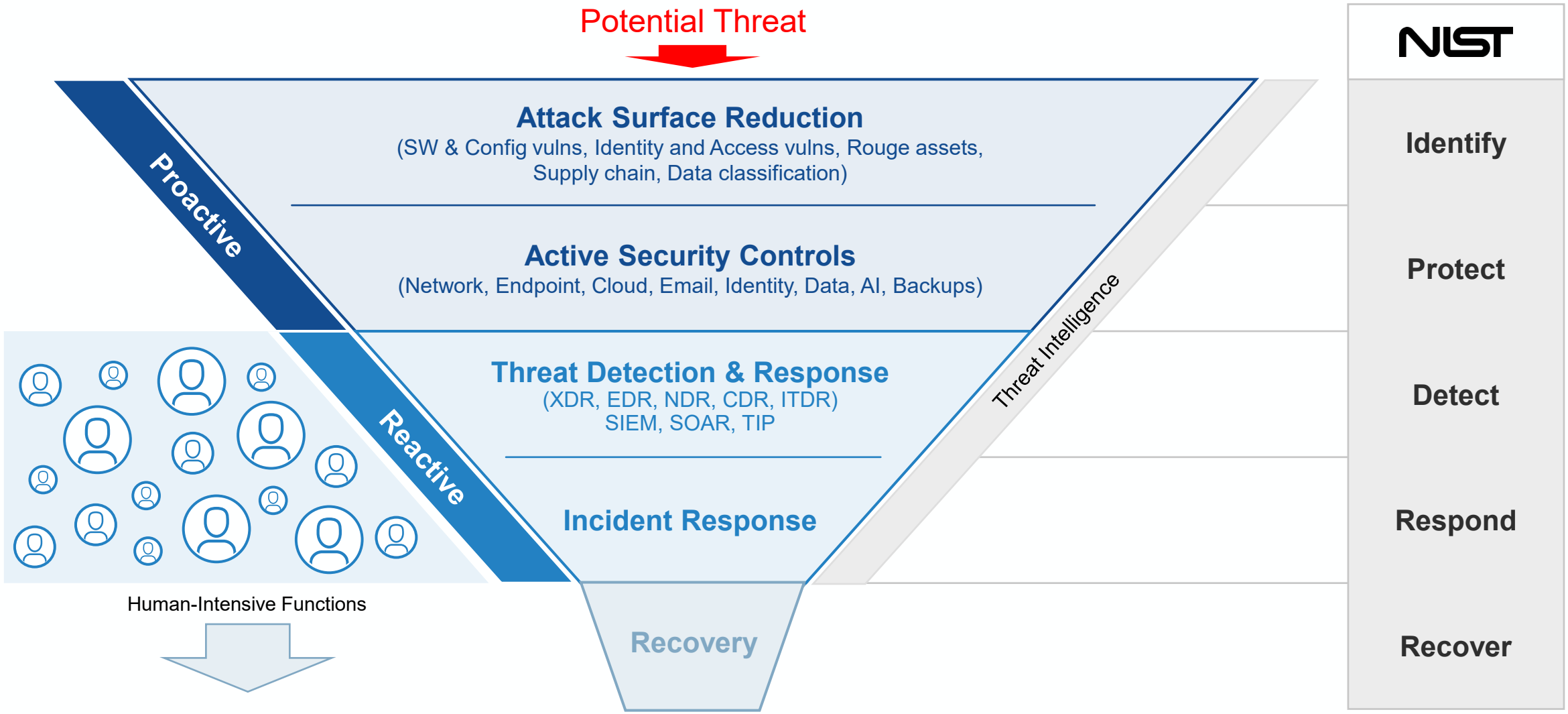
Information Classification: General
©TechTarget, Inc. or its subsidiaries

RSAC™ 2025 Conference

Proactive vs. Reactive

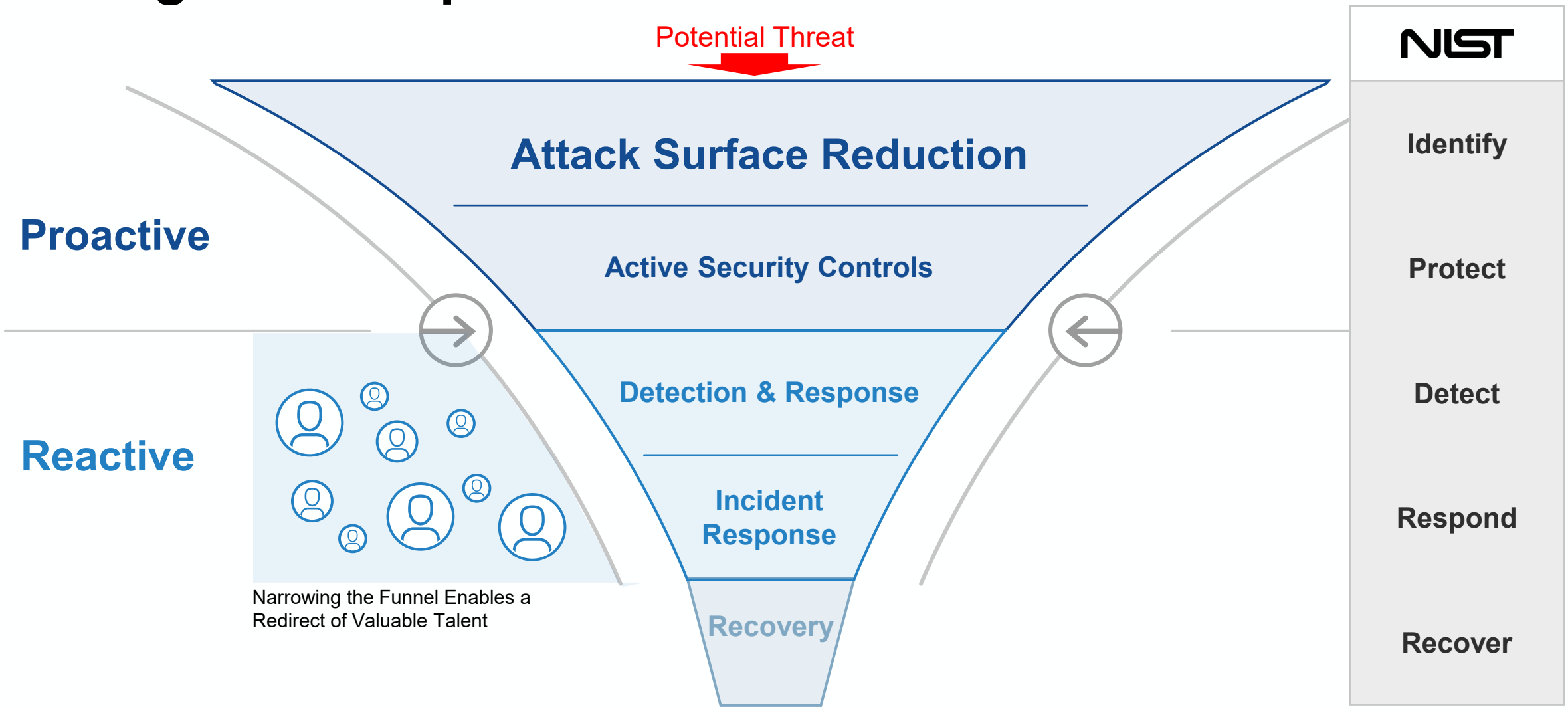
Many Voices.
One Community.

Security Strategies and The Threat Funnel



©TechTarget, Inc. or its subsidiaries

Investments in Proactive Strategies… Change the Shape of the Threat Funnel



©TechTarget, Inc. or its subsidiaries

PRE and POST BOOM

Proactive Risk Reduction

Technology that seeks out and mitigates exposures before they pose a danger to the environment.

Reactive Risk Reduction

Technology that detects, investigates, and remediates threats after or during boom.

"Boom" – The moment when an attack is actively occurring.

STATE

Programmatically address unknown IT assets, vulnerabilities, misconfigurations, and risk.

EVENTS

Programmatically assess runtime and operational risk via active threats in the IT environment.

RSAC 2025 Conference

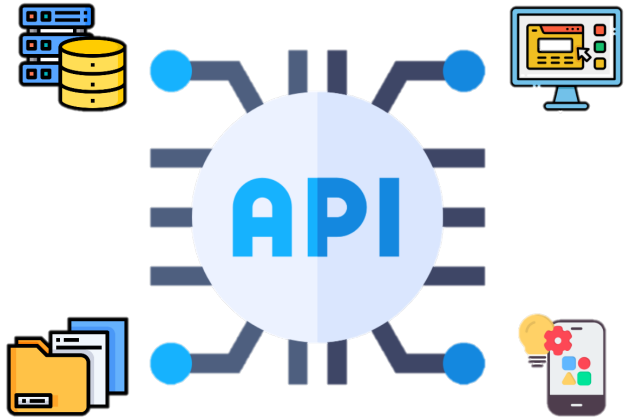
How AI is Impacting These Strategies

Many Voices.
One Community.

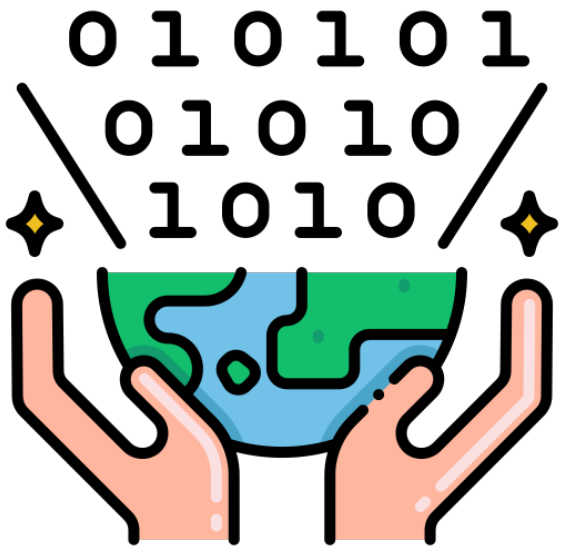
Why Now – What's Changed

What has changed to make the vision of an AI-driven proactive threat and exposure management system possible?

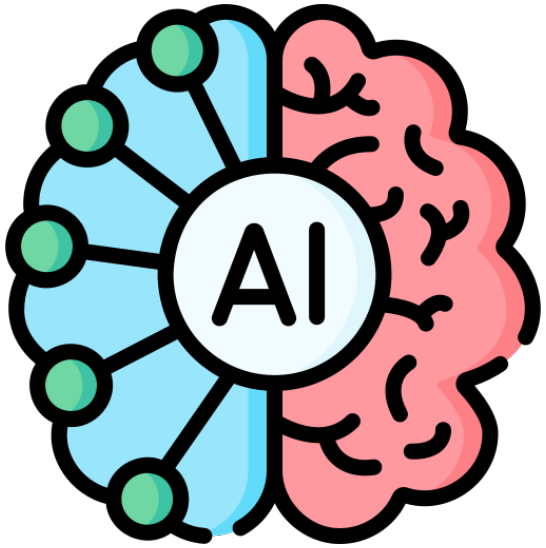
API Driven Ecosystem



Big Data and Cheap Storage



Artificial Intelligence



Attackers Embracing AI

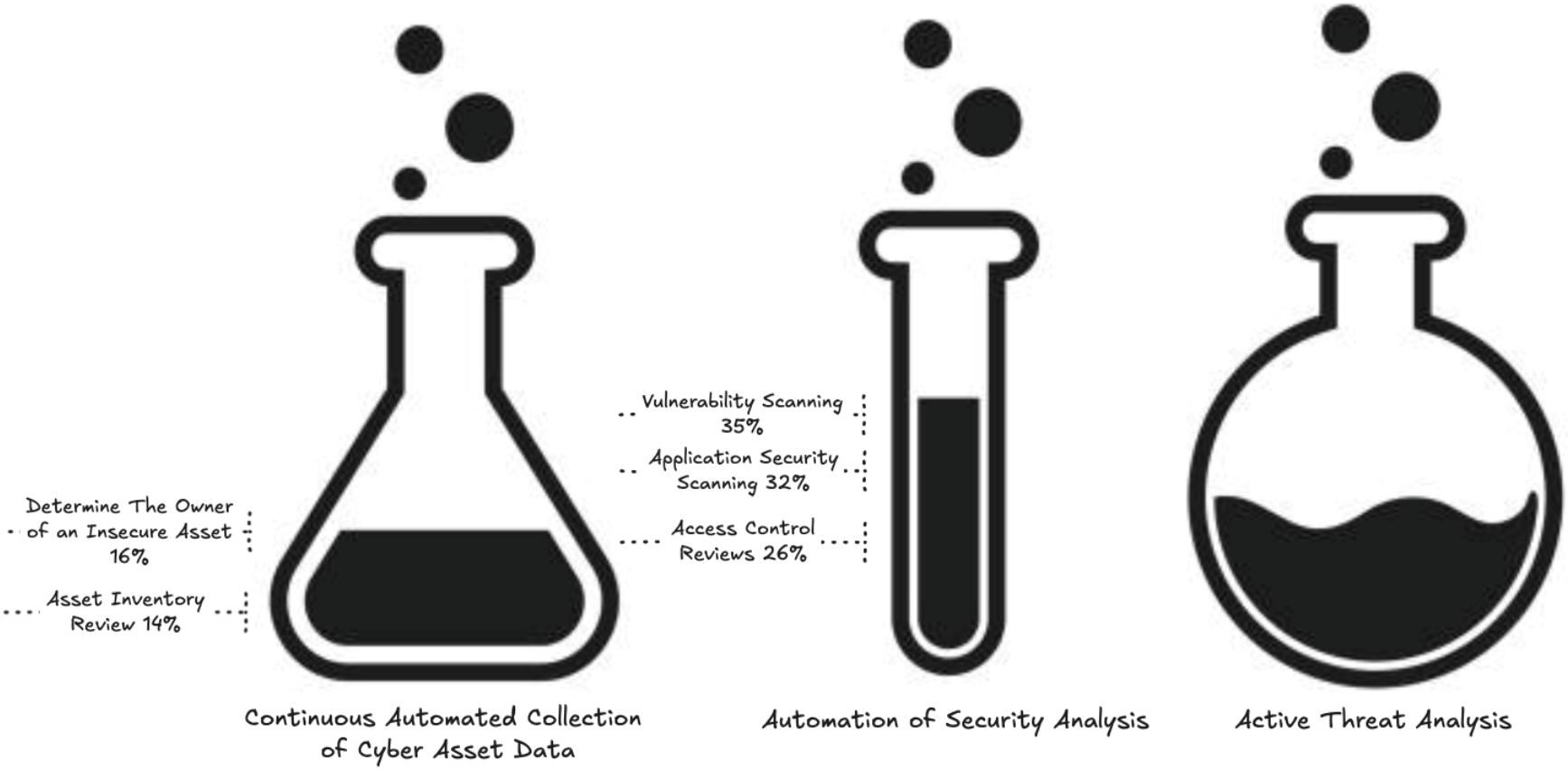
- Automated vulnerability Scanning
- AI generated exploits and weaponization
- Automated malware development and evasion techniques
- Automated and improved social engineering and targeted attack capabilities

- Improved speed and efficiency
- Increased sophistication of attacks
- Evasion improvement
- Increase scale of attacks

Enterprise Strategy Group by TechTarget

©TechTarget, Inc. or its subsidiaries

The Chemistry of a Modern Risk-Based Security Platform


Determine The Owner of an Insecure Asset 16%
Asset Inventory Review 14%
Vulnerability Scanning 35%
Application Security Scanning 32%
Access Control Reviews 26%
Threat Modeling 18%
Continuous Automated Collection of Cyber Asset Data
Automation of Security Analysis
Active Threat Analysis

Which of the following security activities has your organization automated?
(Percent of respondents, N=359, multiple responses accepted)

AUTOMATION IS PROACTIVE SECURITY

- Security teams are looking for ways to automate.
- Automation of data collection, security analytics, and threat analytics
- Asset inventory and asset ownership is required.
- What about automated remediation…

RSAC™ 2025 Conference

Assets

Vulnerabilities

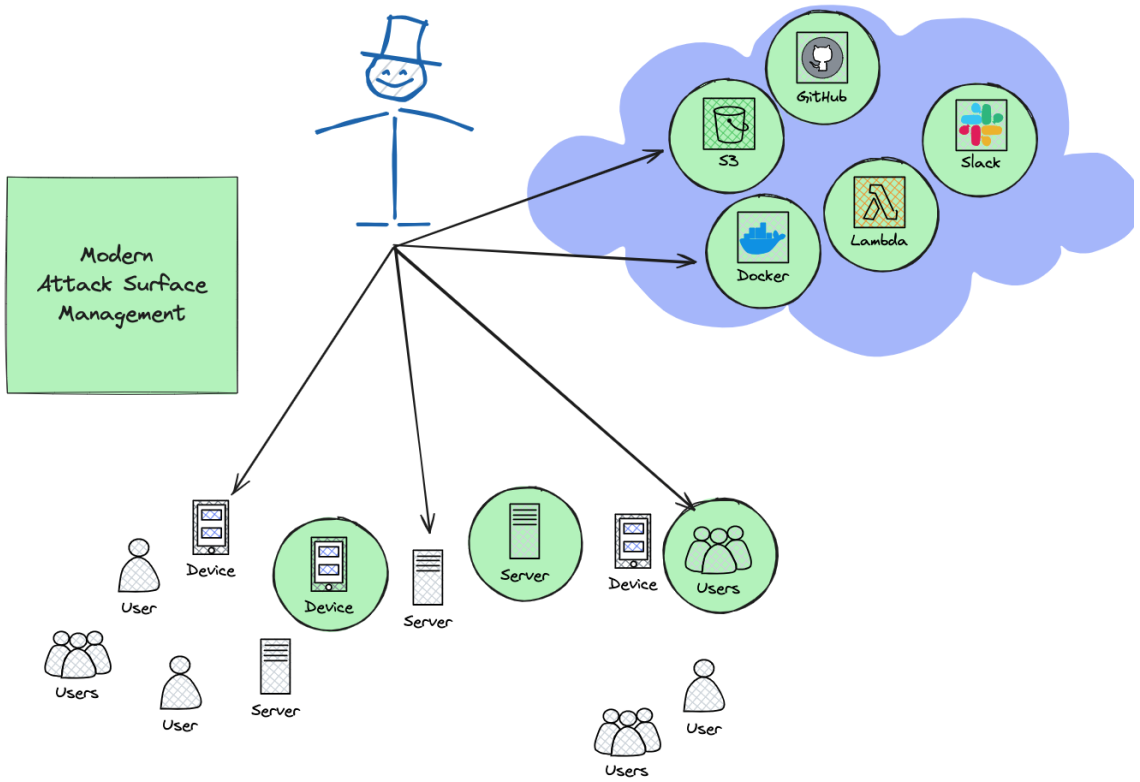
Exposures

Threats

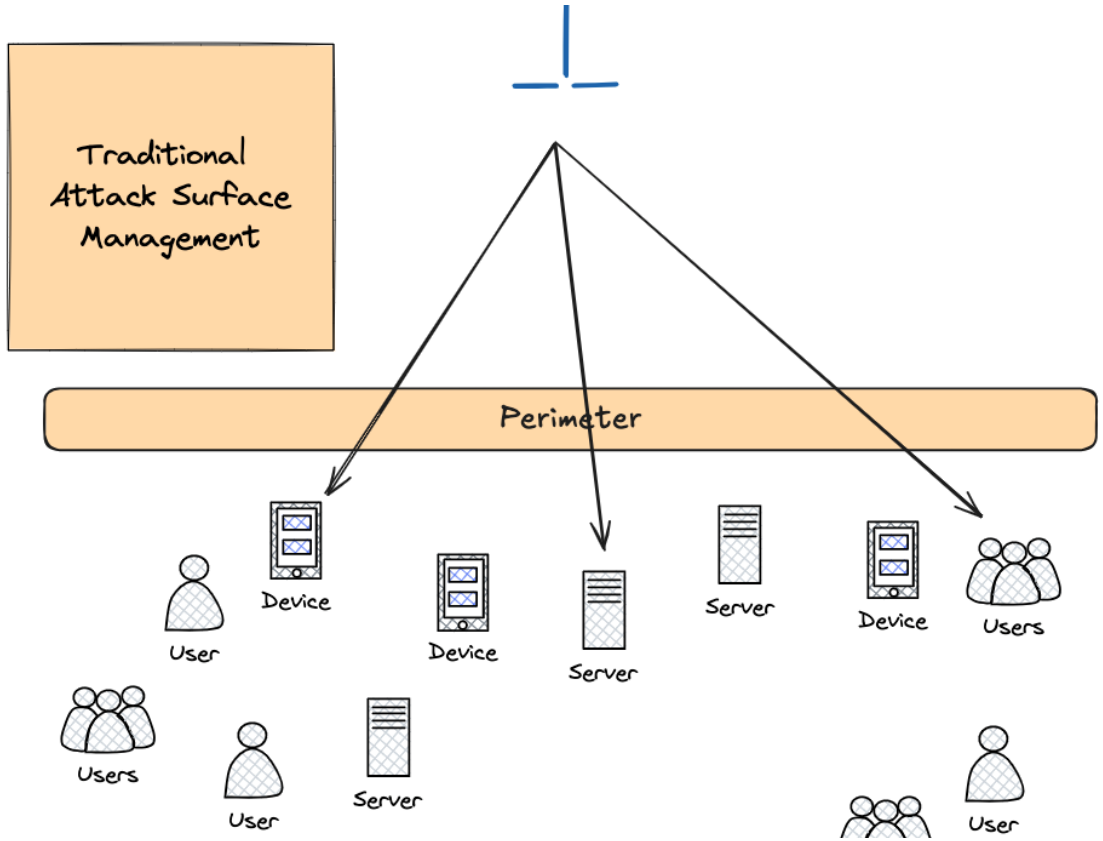
Many Voices.
One Community.

Reconceptualizing The Attack Surface

Micro Perimeter

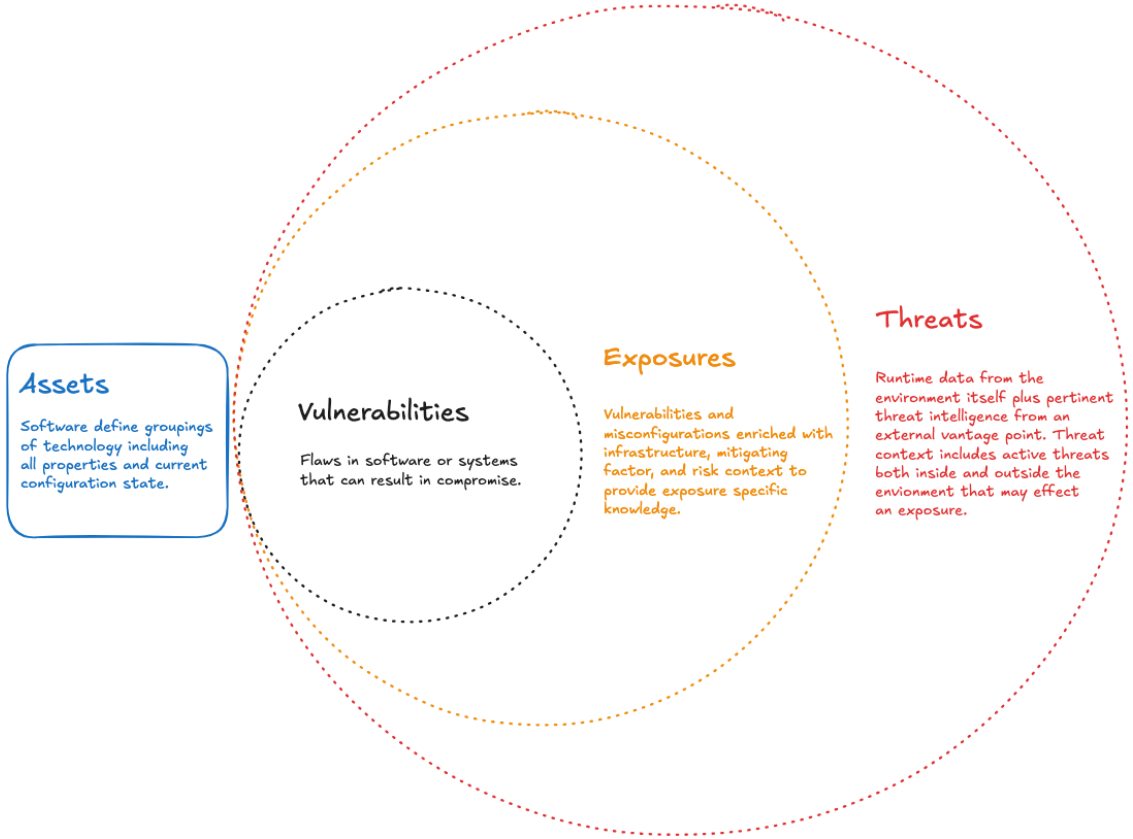


Internal Vs. External



Assets Vulnerabilities Exposures and Threats

- What you have
- What vulnerabilities assets have
- What exposures exist
- What threats exist against your assets


Assets
Software define groupings of technology including all properties and current configuration state.
Vulnerabilities
Flaws in software or systems that can result in compromise.
Exposures
Vulnerabilities and misconfigurations enriched with infrastructure, mitigating factor, and risk context to provide exposure specific knowledge.
Threats
Runtime data from the environment itself plus pertinent threat intelligence from an external vantage point. Threat context includes active threats both inside and outside the enviornment that may effect an exposure.

Assets Vulnerabilities Exposures and Threats

- Define assets that matter to you
- Define assets that matter to risk measurement
- Asset data must include ALL properties and current configuration state
- Track assets continuously
- Track assets programmatically
- Must be automated

Assets Vulnerabilities Exposures and Threats

- First party or third-party problems
- Often a result of bad coding (yours or someone else's)
- Third party inherited risk – bringing in third party vulnerabilities
- Often a supply chain problem
- Notoriously difficult to discover

Assets Vulnerabilities Exposures and Threats

- Superset of vulnerabilities
- Includes misconfigurations and other mistakes resulting in risk
- Enriched with infrastructure, mitigating factor, and risk context.
- Exposures are measured in potential risk impact

Exposures
Vulnerabilities and misconfigurations enriched wit infrastructure, mitigating factor, and risk context to provide exposure specific knowledge.

Assets Vulnerabilities Exposures and Threats

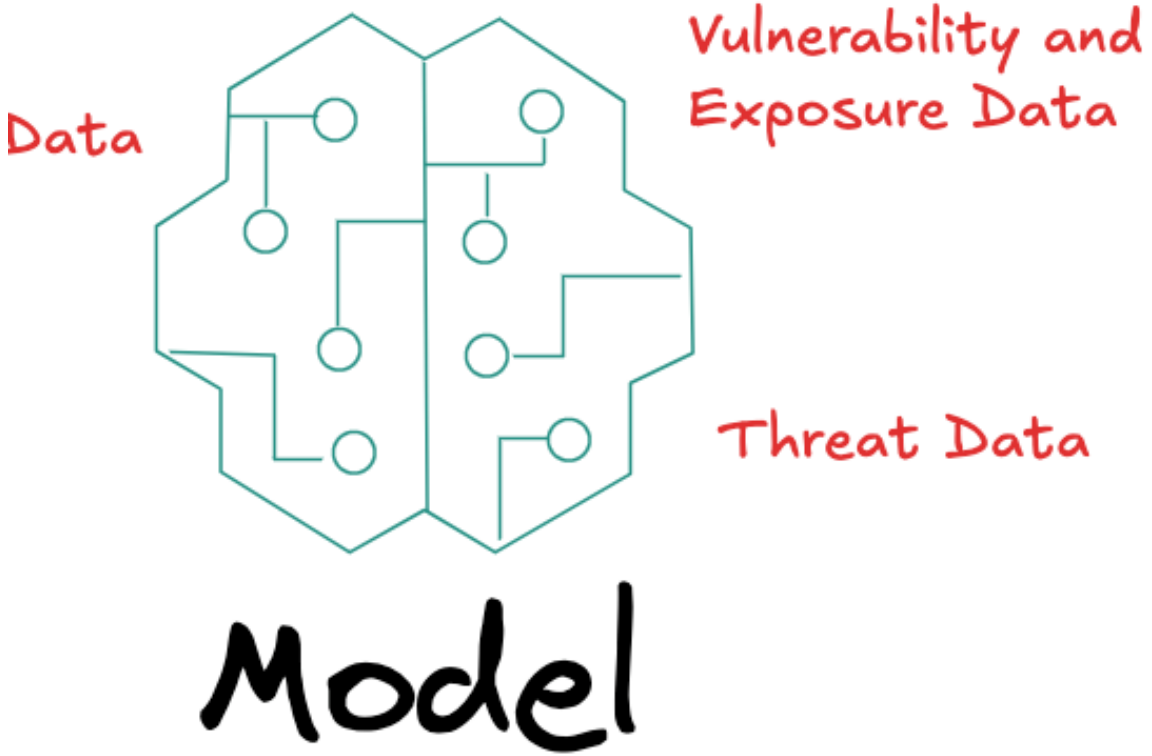
- External and internal
- Active or potential
- Runtime data provides “inside” vantage point
- Threat intelligence and attack surface management provides ”outside” vantage point

Threats

Runtime data from the environment itself plus pertinent threat intelligence from an external vantage point. Threat context includes active threats both inside and outside the envionment that may effect an exposure.

Asset + Exposure / Vulnerability + Threat Data = CONTEXT

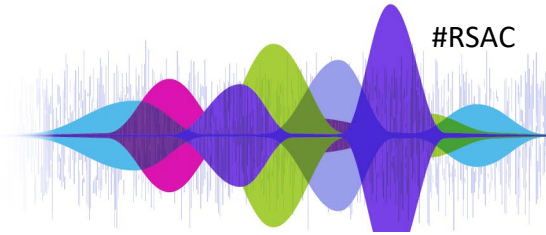
- Comprehensive Mitigation Capabilities
- Asset Value Provides Loss Metrics
- Contextualized Prioritization
- Attack Path Analysis
- Active Threat Risk Elevation
- Automated Contextual Remediation



RSAC™ 2025 Conference

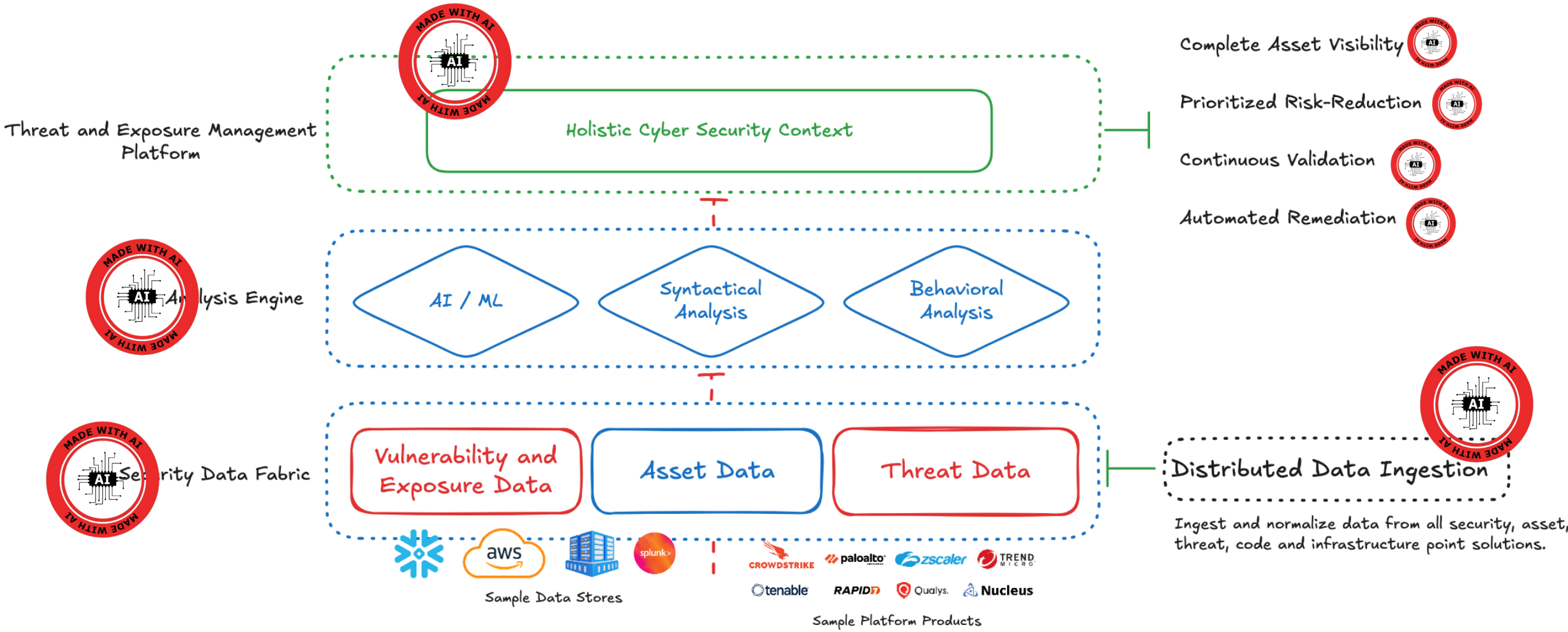
The Threat and Exposure Management Platform

The Threat and Exposure Management Platform



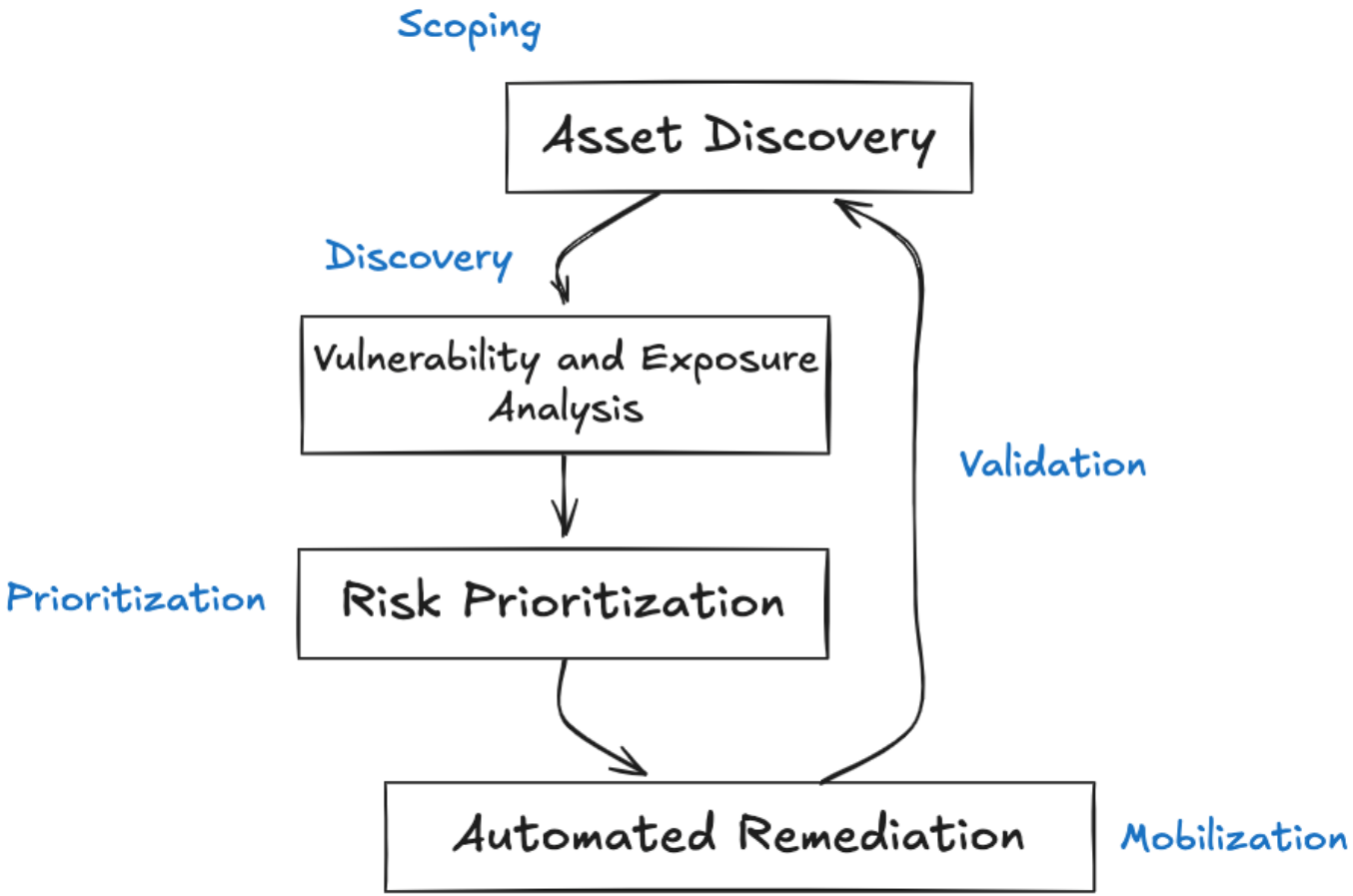
©TechTarget, Inc. or its subsidiaries

The Threat and Exposure Management Platform



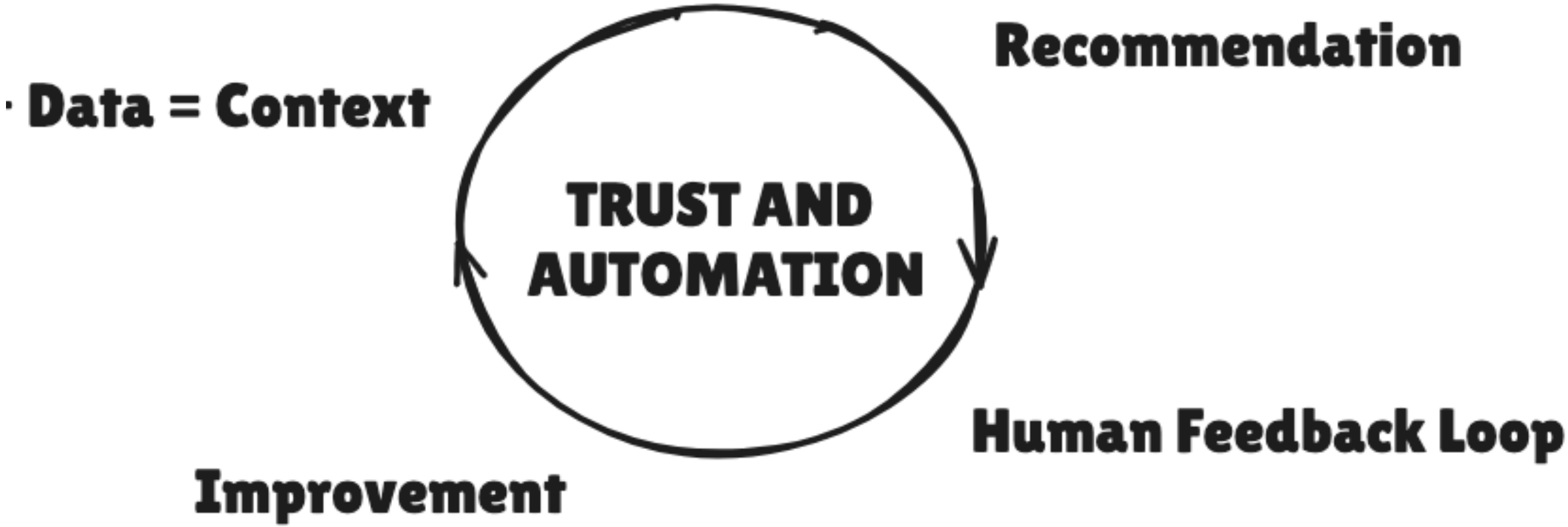
©TechTarget, Inc. or its subsidiaries

Mapping To The CTEM Process



©TechTarget, Inc. or its subsidiaries

Human + AI Contextual Requires A Feedback Loop



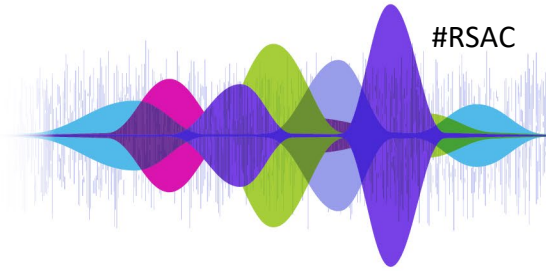
©TechTarget, Inc. or its subsidiaries

RSAC 2025 Conference

Future Outlook and Recommendations

Many Voices.
One Community.

Apply What You've Learned



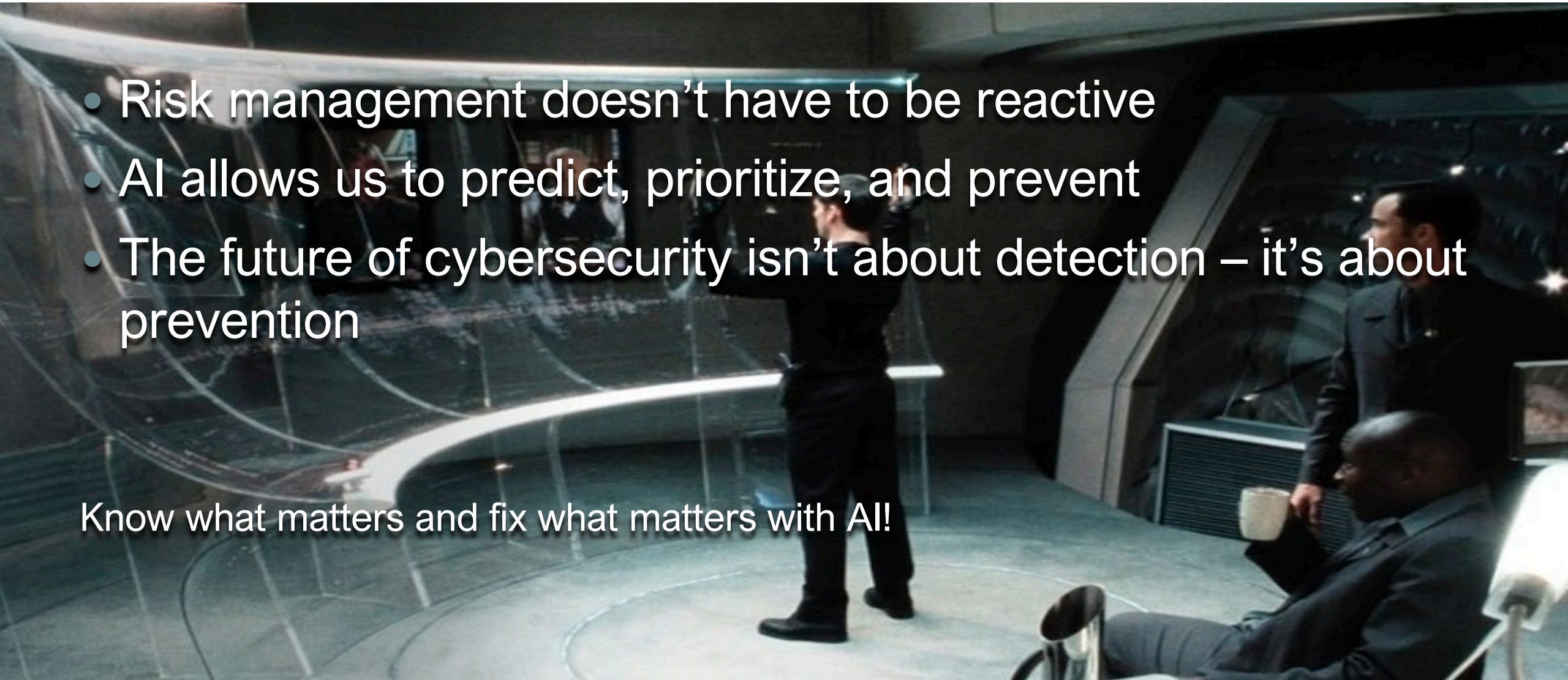
Quick Wins:

- Inventory crown-jewel assets
- Establish real-time visibility on exposures
- Integrate business context into prioritization
- Find what you didn't know about!

Long-Term Strategy:

- Automate contextual remediation
- Build feedback loops into your AI/analytics
- Align risk metrics to board-level outcomes
- Success here isn't about boiling the ocean—it's about building momentum, step by step.

The Future is Predictive



- Risk management doesn't have to be reactive
- AI allows us to predict, prioritize, and prevent
- The future of cybersecurity isn't about detection – it's about prevention

Know what matters and fix what matters with AI!

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you

Tyler Shields

Dave Gruber